Aiello 1999-0053

IN THE CLAIMS

1. (Currently Amended) A method of provisioning a user's broadband telephony interface comprising, in order, the steps of:

receiving information authenticating to the user's broadband telephony interface a provisioning server;

establishing a communication channel between the user and the provisioning server over which is transmitted authorization information from the user to the provisioning server; and

encrypting and transmitting a cryptographic key associated with the user to the provisioning server.

2. (Previously Presented) The method of claim 34 further comprising the step of establishing a voice connection between said user and said network.

3. (Previously Presented) The method of claim 2 further comprising said provisioning server sending a request to said user, over said voice connection, encrypted with said complement of said key AK.

4. (Previously Presented) The method of claim 2 wherein the communication channel passes through said BTI.

5. (Previously Presented) The method of claim 4 wherein said key of said provisioning server is a public key.

6. (Currently Amended) The method of claim 5 wherein said acknowledgement is encrypted with said complement of said key SK.

7. (Previously Presented) The method of claim 6 wherein a random nonce is included in said tuple.

Aiello 1999-0053

8. (Previously Presented) The method of claim 34 wherein the information that authenticates the provisioning server is a digital certificate.

9. (Previously Presented) The method of claim 34 wherein any number of said keys taken from the set consisting of K, AK, and SK are symmetric keys, where a symmetric key is equal to its complement.

10. (Previously Presented) The method of claim 34 wherein said complement of said key K is a public key and said key K is a private key.

11. (Previously Presented) The method of claim 34 wherein a hash is included with each transmission.

12. (Currently Amended) Apparatus comprising:

a first interface to a landline user telephone;

a second interface to a communication network with access to a provisioning server;

memory for storing cryptographic keys;

a processor connected to the memory and the first and second interfaces for executing program instructions, the program instructions causing the processor to perform, in order, the steps of:

receiving a key of said provisioning server and information authenticating the provisioning server to said user telephone;

generating a random key K and its complement, a random session key SK and its complement, and a random audio channel key AK and its complement, where a complement of a key J is a key that decrypts messages message encrypted with said key J; and

sending to said provisioning server information that includes said complement of said K encrypted with said key of said provisioning server, and a tuple encrypted with said K, which tuple includes said complement of said SK, and said complement of said AK.

13. (Previously Presented) The apparatus of claim 12 wherein the processor also generates a public/private key pair, and sends the public key to said provisioning server.

14. (Previously Presented) The apparatus of claim 12 wherein the processor establishes a session communication channel with said provisioning server.

15. (Previously Presented) The apparatus of claim 14 wherein the processor communicates with said provisioning server over said session communication channel by sending messages encrypted with said key SK, and receiving messages encrypted with said complement of said key SK.

16. (Canceled).

17. (Canceled).

18. (Previously Presented) The apparatus of claim 17 wherein a random nonce is included in said tuple.

19. (Previously Presented) The apparatus of claim 12 wherein the information authenticating the provisioning server is a digital certificate.

20. (Previously Presented) The apparatus of claim 12 wherein the key K a symmetric key.

21. (Canceled).

22. (Original) The broadband telephony interface of claim 12 wherein a hash is included with each transmission.

Aiello 1999-0053

23 - 33. (Canceled).

34. (Currently Amended) A method of employing a user's broadband telephony interface (BTI), executed in said BTI in communication with a network, comprising, in order, the steps of:

sending a request to a provisioning server;

receiving a message that includes a key of said provisioning server and information that authenticates said provisioning server to said user's BTI;

generating a random key K and its complement, a random session key SK and its complement, and a random audio channel key AK and its complement, where a complement of a key J is a key that decrypts messages message encrypted with said key J;

sending a message to said provisioning server information that includes said complement of said K encrypted with said key of said provisioning server, and a tuple encrypted with said K, which tuple includes said complement of said SK, and said complement of said AK; and

receiving an acknowledgement from said provisioning server.

35. (Previously Presented) The method of claim 3 further comprising the steps of:

relaying said request to said user;

receiving responsive information from said user; and

forwarding said responsive information to said provisioning server, encrypted with said key AK.

36. (Previously Presented) The method of claim 35 further comprising the steps of:

generating a public/private key pair; and

sending the generated public key to said provisioning server, encrypted with said key SK.

37. (Previously Presented) The method of claim 36 further comprising the step of receiving an acknowledgement message from said provisioning server, in response to said sending of the generated public key, which acknowledgement message is encrypted with said complement of said key SK.

38. (Previously Presented) The method of claim 34 wherein said step of sending to said provisioning server includes information encrypted with said key SK.

39. (Previously Presented) The method of claim 38 wherein said information encrypted with said key SK provides an address of said BTI.